SHADOW IT
CHALLENGES IN LIGHT OF THE
CIS CRITICAL SECURITY CONTROLS

https://www.cisecurity.org/controls

01. Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise [...] and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Why is this Control critical?
Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

Shadow IT Challenge & Solution

Third-party web accounts and identities created by employees are invisible on the local network, as well as from network or endpoint logs. Targeted discovery of accounts is not viable via traffic inspections as remote workers may not always connect to central proxies, and SSL decryption is done via purpose-built perimeter tools that are not designed to capture account and log-in details which may not be easy to find from such data anyway. Complete capture of such traffic may also come at high costs and violate privacy rights when private traffic is being decrypted for complete logging.

Scirge provides policy-based discovery for third-party accounts and applications via identifying corporate email addresses when used to log in or create new accounts on any website or web application. This establishes an accurate inventory without relying on inspecting large amounts of network or endpoint logs, and without the potential of breaching individual privacy rights.

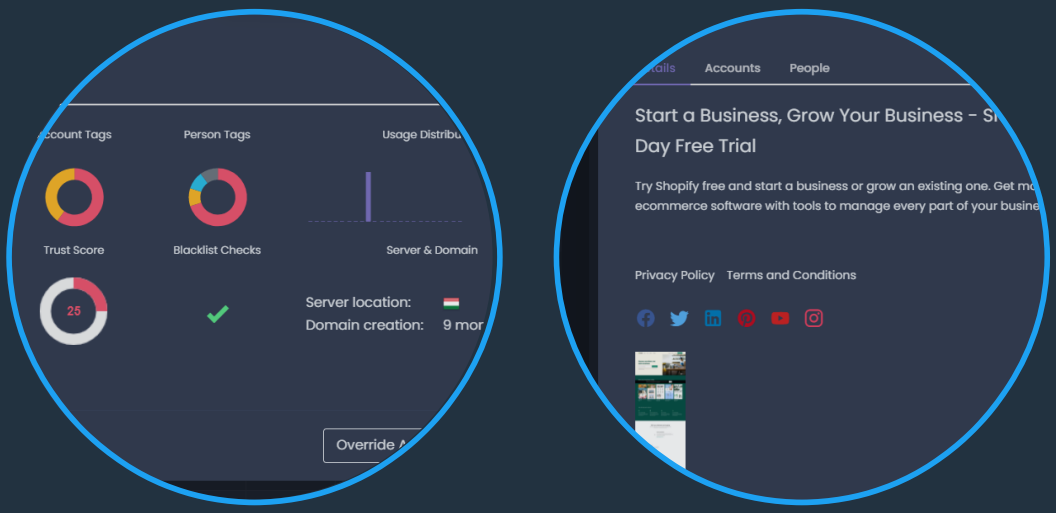
03. Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Why is this Control critical?
Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world.

Shadow IT Challenge & Solution

Shadow IT cloud applications may handle and process data the same way as any local software. CIS requires you to define and inventory, access rights, retention, disposal, and encryption amongst others. Third-party applications are no exception. Their geographical location, encryption, authentication methods, SLAs, and Terms and Conditions about how they use your data are essential to keep track of.



"The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem [...] with every role [...] and across many sectors [...] who have banded together to create, adopt, and support the CIS Controls."

Scirge enumerates applications along with their metadata, such as their Privacy Policies, geo-data, risk scores, and the employees that access them. This allows compliance departments to review apps that have the potential to store or process sensitive data, and create awareness or policies for their proper use. As logs and direct integrations are not possible with all third-party providers, employee awareness, visibility, and compliance policies are the only possible route to properly address data management in these services.

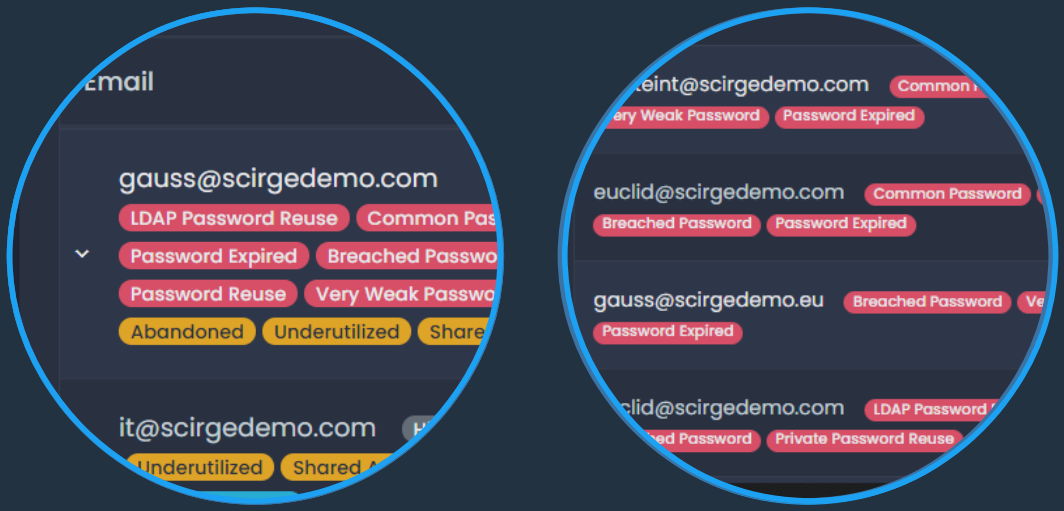
05. Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Why is this control critical?
It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), social engineering a user to give their password, or using malware to capture passwords or tokens in memory or over the network.

Shadow IT Challenge & Solution

Passwords created and used in Shadow IT applications are not managed by IT organizations and therefore cannot be integrated with central PAM or other identity-related services. Multi-factor and SSO services are not always available, and they are provided in an opt-in manner, similarly to password managers, and are thus reliant on your employee's security education and awareness levels. Enterprise password complexities are not enforced and employees leaving the organizations may also retain access rights to these services for a very long time.



Scirge rigorously checks all third-party passwords for weaknesses and desired complexities, as well as contextual passwords relating to the organization. Secure hashes of every password used are compared to known breach lists as well as important local directory passwords. Shared and unused accounts are pinpointed, and personal level inventories are created to provide the ability to revoke important rights when employees leave the organization. Employees may be warned immediately when at risk, such as using weak credentials, and for the proper use of available MFA or SSO methods depending on the application.

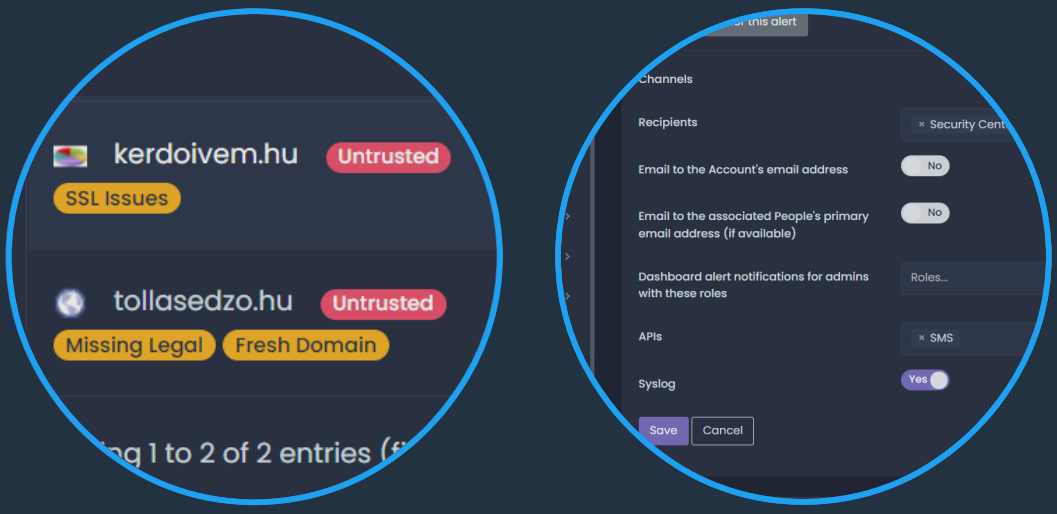
09. Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Why is this control critical?
Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data, or providing an open channel to allow attackers to gain access, thus increasing risk to the enterprise.

Shadow IT Challenge & Solution

More than 10,000 new generic top-level domains are registered every hour. This poses a challenge for perimeter protection tools such as email filters or firewalls/proxies, as they rely on databases that cannot get updated at such a high pace. 77% of phishing attacks are launched from domains that are less than three months old, and stolen credentials are utilized within a few hours after a successful phishing attack. When both employees and perimeter security tools fail to identify such an attempt, there are no indicators of compromise available. This is especially true in case these stolen credentials are used to target other third-party applications, without authentication logs or any level of visibility for security departments.



Protecting against phishing requires the correlation of website metadata, such as domain age, SSL configuration, and other DNS settings, with the fact that a corporate login or password reuse had been conducted on it. Scirge utilizes its proprietary Horizon Cloud Intelligence service to provide phishing detection once they had been successful, and alerts the employee as well as security departments within minutes.

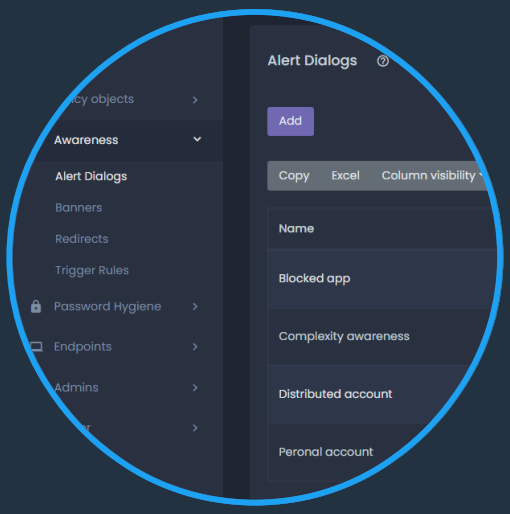
14. Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Why is this control critical?
Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public sites.

Shadow IT Challenge & Solution

Shadow IT is good for business. Agile employees and business units are independently solving day-to-day operational tasks and use third-party services regularly for productivity. Training on policies and best practices is rare and contains a high volume of information that is hard to digest and cumbersome to follow for non-IT experts. The high risks associated with Shadow IT applications and accounts are usually not paired with a focused and continuous training approach.



Scirge provides action-based awareness right when employees are at risk, utilizing the primary real estate of their daily focus, the web browser. Policy-based awareness messages such as pop-ups redirects show only when relevant and may be customized for different job roles or business units. Additional follow-up messages in the forms of email, SMS, or any other channel may be set up to remind about overdue password changes, breached accounts, or any other important activities that they may need to take in order to protect the organization. Awareness messages may also be set up based on the correlation of events, such as sharing of accounts, phishing attempts, or emerging trends.